

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 2001016197 A

(43) Date of publication of application: 19.01.01

(51) Int. Cl. H04L 9/26
G09C 1/00

(21) Application number: 11187699

(71) Applicant: TOYO COMMUN EQUIP CO LTD

(22) Date of filing: 01.07.99

(72) Inventor: SUGIMOTO KOICHI

(54) SELF-SYNCHRONIZED STREAM ENCIPHERING SYSTEM AND MAC GENERATING METHOD USING THE SAME

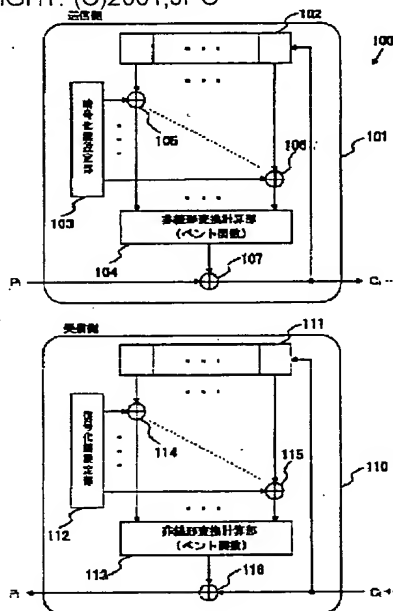
(57) Abstract:

PROBLEM TO BE SOLVED: To provide a self-synchronized stream enciphering system with which the mutual correlation of the sequence obtained by deciphering the cipher text, generated by a certain key, by using another key is extremely small in comparison with the sequence of plaintext and key setting is made easy.

SOLUTION: In a self-synchronized stream enciphering device 100 for inputting the plaintext bit by bit and outputting the cipher text bit by bit and having plural steps of shift registers 102, a nonlinear transformation calculating part 104 of multi-bit input and one-bit output and an encipher key setting part 103 for storing an encipher key, the nonlinear transformation calculating part 104 is provided with a bent function operating part for inputting the result of exclusively ORing the value in the shift register 102 and the setting value of the encipher key setting part 103 for each bit and outputting the operation result of a corresponding

bent function and the result obtained by exclusively ORing the plaintext and the output of the non-linear conversion calculating part 104 for each bit is successively inputted to the shift register 102 and defined as a cipher text to be outputted.

COPYRIGHT: (C)2001,JPO



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-16197

(P2001-16197A)

(43) 公開日 平成13年1月19日 (2001.1.19)

(51) Int.Cl. ⁷	識別記号	F I	テームト (参考)
H 0 4 L 9/26		H 0 4 L 9/00	6 5 9 5 J 1 0 4
G 0 9 C 1/00	6 1 0	G 0 9 C 1/00	6 1 0 D
	6 4 0		6 4 0 D

審査請求 未請求 請求項の数 6 O L (全 8 頁)

(21) 出願番号 特願平11-187699

(22) 出願日 平成11年7月1日 (1999.7.1)

(71) 出願人 000003104

東洋通信機株式会社

神奈川県高座郡寒川町小谷2丁目1番1号

(72) 発明者 杉本 浩一

神奈川県高座郡寒川町小谷2丁目1番1号

東洋通信機株式会社内

(74) 代理人 100098039

弁理士 遠藤 恭

Fターム(参考) 5j104 AA01 AA08 JA06 LA02 NA02

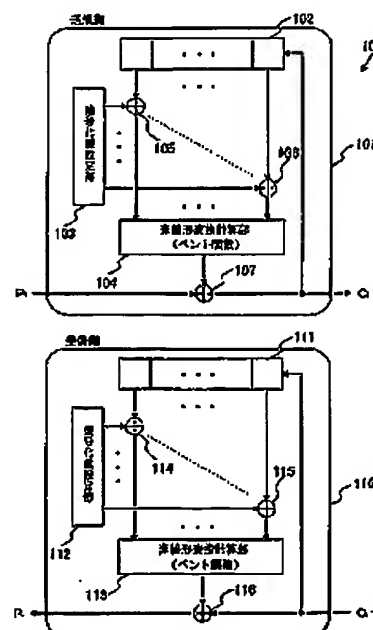
NA08 NA23 NA37

(54) 【発明の名称】 自己同期型ストリーム暗号システム及びこれを用いたMAC生成方法

(57) 【要約】

【課題】 ある鍵によって生成された暗号文の系列を異なる鍵で復号した場合の系列が、平文の系列と比較した場合、その相互相関が極めて小さくなり、かつ、鍵の設定が容易であるような自己同期型ストリーム暗号システムを提供する。

【解決手段】 本発明は、複数段のシフトレジスタ102と、多ビット入力1ビット出力の非線形変換計算部104と、暗号化鍵を格納する暗号化鍵設定部103とを有し、平文を1ビットずつ入力し暗号文を1ビットずつ出力する自己同期型ストリーム暗号の暗号化装置100であって、非線形変換計算部104が、シフトレジスタ102における値と暗号化鍵設定部103の設定値をビット毎に排他的論理和した結果を入力とし、これに対するベント関数の演算結果を出力とするベント関数演算部を備え、前記平文と非線形変換計算部104の出力をビット毎に排他的論理和した結果を、シフトレジスタ102へ順次入力すると共に、出力される暗号文とする。



(2)

特開2001-16197

1

2

【特許請求の範囲】

【請求項1】 同期信号に同期して動作する複数段のシフトレジスタと、多ビット入力1ビット出力の非線形変換計算部と、 n ビットの暗号化鍵を格納する暗号化鍵設定部とを有し、前記同期信号に同期して、平文を1ビットずつ入力し、暗号文を1ビットずつ出力する自己同期型ストリーム暗号の暗号化装置であって、

前記非線形変換計算部が、前記シフトレジスタにおけるレジスタ n ビットと前記暗号化鍵設定部に設定された暗号化鍵 n ビットをビット毎に排他的論理和演算した結果を少なくともその入力とし、該入力に対しベント関数による演算を行った結果を出力とするベント関数演算部を備え、

前記入力された平文と前記非線形変換計算部の出力をビット毎に排他的論理和演算した結果を、前記シフトレジスタへ順次入力すると共に、前記出力される暗号文としたことを特徴とする自己同期型ストリーム暗号の暗号化装置。

【請求項2】 同期信号に同期して動作する複数段のシフトレジスタと、多ビット入力1ビット出力の非線形変換計算部と、 n ビットの復号化鍵を格納する復号化鍵設定部とを有し、前記同期信号に同期して、暗号文を1ビットずつ入力し、復号文を1ビットずつ出力する自己同期型ストリーム暗号の復号化装置であって、

前記非線形変換計算部が、前記シフトレジスタにおけるレジスタ n ビットと前記復号化鍵設定部に設定された復号化鍵 n ビットをビット毎に排他的論理和演算した結果を少なくともその入力とし、該入力に対しベント関数による演算を行った結果を出力とするベント関数演算部を備え、

前記入力された暗号文を、前記シフトレジスタへ入力すると共に、前記入力された暗号文と前記非線形変換計算部の出力をビット毎に排他的論理和演算した結果を、前記出力される復号文としたことを特徴とする自己同期型ストリーム暗号の復号化装置。

【請求項3】 請求項1記載の自己同期型ストリーム暗号の暗号化装置と請求項2記載の自己同期型ストリーム暗号の復号化装置を備えて構成される自己同期型ストリーム暗号システム。

【請求項4】 請求項1記載の自己同期型ストリーム暗号の暗号化装置を用いて N ビットの平文から S ビットのメッセージ認証子を生成するMAC生成方法であって、前記シフトレジスタに所定の初期値を設定する手順と、前記暗号化装置に N ビットの平文を入力する手順と、前記暗号化装置から出力された N ビットの暗号文の末尾から連続する S ビットをメッセージ認証子として出力する手順と、を備えたことを特徴とするMAC生成方法。

【請求項5】 同期信号に同期して動作する複数段のシフトレジスタと、多ビット入力1ビット出力の非線形変換計算部と、 n ビットの暗号化鍵を格納する暗号化鍵設

定部とを有し、前記同期信号に同期して、平文を1ビットずつ入力し、暗号文を1ビットずつ出力する自己同期型ストリーム暗号の暗号化方法であって、前記入力された平文と前記非線形変換計算部の出力をビット毎に排他的論理和演算する手順と、

前記排他的論理和演算の結果を、前記シフトレジスタへ順次入力すると共に、前記出力される暗号文として用いる手順と、

前記シフトレジスタにおけるレジスタ n ビットと前記暗号化鍵設定部に設定された暗号化鍵 n ビットをビット毎に排他的論理和演算する手順と、

前記排他的論理和演算の結果を少なくともその入力とし、該入力に対しベント関数による演算を行う手順と、前記ベント関数による演算の結果を含んで前記非線形変換計算部の出力を生成する手順と、を備えた自己同期型ストリーム暗号の暗号化方法。

【請求項6】 同期信号に同期して動作する複数段のシフトレジスタと、多ビット入力1ビット出力の非線形変換計算部と、 n ビットの復号化鍵を格納する復号化鍵設定部とを有し、前記同期信号に同期して、暗号文を1ビットずつ入力し、復号文を1ビットずつ出力する自己同期型ストリーム暗号の復号化方法であって、

前記入力された暗号文を、前記シフトレジスタへ順次入力する手順と、

前記シフトレジスタにおけるレジスタ n ビットと前記復号化鍵設定部に設定された復号化鍵 n ビットをビット毎に排他的論理和演算する手順と、

前記排他的論理和演算の結果を少なくともその入力とし、該入力に対しベント関数による演算を行う手順と、前記ベント関数による演算の結果を含んで前記非線形変換計算部の出力を生成する手順と、

前記入力された暗号文と前記非線形変換計算部の出力をビット毎に排他的論理和演算し、その結果を、前記出力される暗号文として用いる手順と、を備えた自己同期型ストリーム暗号の復号化方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、暗号通信装置などで利用される自己同期型ストリーム暗号システム、及び該システムを用いたMAC生成方法に関する。

【従来の技術】従来より、電話機、無線通信装置、データ通信装置のような通信システムにおいては、第三者、すなわちその通信システムの両端の通信当業者以外の者が、その通信システムで伝送される情報を知ることができないようにするために、ここで伝送される伝送情報を暗号化することが行われている。

【0002】この暗号化の方式としては多種の方式が知られているが、高速なデータ通信に利用可能な方式としてはストリーム暗号方式がある。図4に沿って、ストリーム暗号方式の一形態である自己同期型ストリーム暗号

(3)

特開2001-16197

3

4

方式について説明する。

【0003】図において、自己同期型ストリーム暗号システム400は、データストリーム（平文）を暗号化する自己同期型ストリーム暗号化装置401（送信側）および暗号化されたストリーム（暗号文）を復号化する自己同期型ストリーム復号化装置405（受信側）を備える。暗号化装置401と復号化装置405は、それぞれ同じ構造のシフトレジスタ402、406、非線形変換計算部403、407を有する。

【0004】すなわち、暗号化装置401は、シフトレジスタ402、非線形変換計算部403及び排他的論理和演算部404を備える。暗号化装置401では、平文 P_i がビット毎に入力されると、同期信号に同期して暗号文 C_i がビット毎に出力される。すなわち、平文 P_i と非線形変換計算部403の出力は、排他的論理和演算部404でビット毎に排他的論理和演算され、その結果は、暗号文 C_i として出力されると共に、シフトレジスタ402の最右段に入力される。シフトレジスタ402は同期信号に同期してその記憶している内容を1ビット左シフトする。非線形変換計算部403はシフトレジスタ402の各段におけるレジスタ値を非線形変換し、結果の1ビットを出力する。

【0005】復号化装置405は、シフトレジスタ406、非線形変換計算部407及び排他的論理和演算部408を備える。復号化装置405では、暗号化装置401から送信された暗号文 C_i がビット毎に入力されると、同期信号に同期して平文 P_i がビット毎に出力される。すなわち、暗号文 C_i と非線形変換計算部407の出力は、排他的論理和演算部408でビット毎に排他的論理和演算され、その結果は、平文 P_i として出力される。同時に暗号文 C_i は、シフトレジスタ406の最右段に入力される。シフトレジスタ406は、同期信号に同期してその記憶している内容を1ビット左シフトする。非線形変換計算部407はシフトレジスタ406の各段におけるレジスタ値を非線形変換し、結果の1ビットを出力する。

【0006】次に、前記自己同期型ストリーム暗号システムを用いたMAC生成方法について説明する。MAC (Message Authenticate Codes: メッセージ認証子)は、暗号化鍵に依存して、平文の特徴を抽出したデータであり、元の平文データの改ざんを検出するために利用される。MACは暗号化鍵に依存しているため、暗号化鍵を有しない第三者によって、簡単に生成することができない。MACを付加したデータにおいては、第三者がデータ部分を改ざんしても、MAC部分を算出することが困難である。したがって、第三者によるデータ改ざんを検出することができる。

【0007】暗号化方式を利用すると、簡単にMACを生成することができる。例えば、DES (Data Encryption Standard)などのブロック暗号方式のCBC (Cipher Block Chaining)モードを用いれば、MACは暗号文の

最終ブロックとして算出できることが知られている。

【0008】図5は、ブロック暗号方式におけるCBCモード500を示したものである。符号501はブロック暗号における暗号化部であり、符号503、504はそれぞれサイズの等しい平文ブロック、暗号文ブロックを示している。符号505は1サイクル前の暗号文ブロックである。平文は一定のサイズのブロックに分割され、最初のブロックから順番に503に配置される。暗号文は暗号化部501から出力されたブロック504を順番に並べたものとなる。

【0009】最初の暗号化では、まず、505に初期値が設定される。505に設定された初期値は503に入力された平文ブロックと同位置のビット毎に502において排他的論理和演算され、暗号化部501によって暗号化されて、暗号文ブロック504として出力される。次以降の暗号化では、505には前回出力された暗号文ブロックが設定される。

【0010】上述したCBCモードを用いれば、MACは暗号文の最終ブロックとして得られる。また、図4に示した自己同期型ストリーム暗号では、非線形変換計算部403の出力を図5における暗号文ブロック (C_i) 504と考え、暗号文の最終部分をMACとすることができる。

【0011】

【発明が解決しようとする課題】しかしながら、図4に示した自己同期型ストリーム暗号システムでは、暗号化及び復号化鍵として、非線形変換計算部403、407の構造を共通にする必要があるが、その構造は複雑であるため、暗号化及び復号化鍵として扱いづらいという問題があった。

【0012】また、鍵同士には、ある鍵によって生成された暗号文の系列を異なる鍵で復号した場合の系列と、平文の系列とを比較した場合、その相互相関が極めて小さくなるという性質が要求される。即ち、鍵同士には、復号化鍵が暗号化鍵と異なった場合、平文と全く異なった系列が生じることが必要となる。しかしながら、従来、このような性質をもった非線形変換計算部を鍵として採択する効率的な手法が存在しないといった問題もあった。

【0013】また、従来の自己同期型ストリーム暗号システムでは、鍵の設定が容易ではないため、暗号化鍵に依存したMACの生成も困難であった。

【0014】本発明では、前記問題点に鑑み、ある鍵によって生成された暗号文の系列を異なる鍵で復号した場合の系列が、平文の系列と比較した場合、その相互相関が極めて小さくなり、かつ、鍵の設定が容易であるような自己同期型ストリーム暗号システムを提供することを目的とする。

【0015】また、本発明は、前記自己同期型ストリーム暗号システムを用いたMAC生成方法を提供する。

(4)

特開2001-16197

5

6

【0016】

【課題を解決するための手段】前記目的を達成するため本発明は、同期信号に同期して動作する複数段のシフトレジスタと、多ビット入力1ビット出力の非線形変換計算部と、 n ビットの暗号化鍵を格納する暗号化鍵設定部とを有し、前記同期信号に同期して、平文を1ビットずつ入力し、暗号文を1ビットずつ出力する自己同期型ストリーム暗号の暗号化装置であって、前記非線形変換計算部が、前記シフトレジスタにおけるレジスタ n ビットと前記暗号化鍵設定部に設定された暗号化鍵 n ビットを

10

出力する自己同期型ストリーム暗号の暗号化方法であって、前記入力された平文と前記非線形変換計算部の出力をビット毎に排他的論理和演算する手順と、前記排他的論理和演算の結果を、前記シフトレジスタへ順次入力すると共に、前記出力される暗号文として用いる手順と、前記シフトレジスタにおけるレジスタ n ビットと前記暗号化鍵設定部に設定された暗号化鍵 n ビットをビット毎に排他的論理和演算する手順と、前記排他的論理和演算の結果を少なくともその入力とし、該入力に対しベント関数による演算を行う手順と、前記ベント関数による演算の結果を含んで前記非線形変換計算部の出力を生成する手順と、を備えて構成される。

【0017】本発明はまた、同期信号に同期して動作する複数段のシフトレジスタと、多ビット入力1ビット出力の非線形変換計算部と、 n ビットの復号化鍵を格納する復号化鍵設定部とを有し、前記同期信号に同期して、暗号文を1ビットずつ入力し、復号文を1ビットずつ出力する自己同期型ストリーム暗号の復号化装置であって、前記非線形変換計算部が、前記シフトレジスタにおけるレジスタ n ビットと前記復号化鍵設定部に設定された復号化鍵 n ビットをビット毎に排他的論理和演算した結果を少なくともその入力とし、該入力に対しベント関数による演算を行った結果を出力とするベント関数演算部を備え、前記入力された暗号文を、前記シフトレジスタへ入力すると共に、前記入力された暗号文と前記非線形変換計算部の出力をビット毎に排他的論理和演算した結果を、前記出力される復号文としたことを特徴として構成される。

20

【0021】更に本発明は、同期信号に同期して動作する複数段のシフトレジスタと、多ビット入力1ビット出力の非線形変換計算部と、 n ビットの復号化鍵を格納する復号化鍵設定部とを有し、前記同期信号に同期して、暗号文を1ビットずつ入力し、復号文を1ビットずつ出力する自己同期型ストリーム暗号の復号化方法であって、前記入力された暗号文を、前記シフトレジスタへ順次入力する手順と、前記シフトレジスタにおけるレジスタ n ビットと前記復号化鍵設定部に設定された復号化鍵 n ビットをビット毎に排他的論理和演算する手順と、前記排他的論理和演算の結果を少なくともその入力とし、該入力に対しベント関数による演算を行う手順と、前記ベント関数による演算の結果を含んで前記非線形変換計算部の出力を生成する手順と、前記入力された暗号文と前記非線形変換計算部の出力をビット毎に排他的論理和演算し、その結果を、前記出力される暗号文として用いる手順と、を備えて構成される。

30

【0022】

【発明の実施の形態】以下、図示した一実施形態に基づいて本発明を詳細に説明する。図1は、本発明に係る自己同期型ストリーム暗号システムの一実施形態を示すブロック図である。図において、自己同期型ストリーム暗号システム100は、データストリーム（平文）を暗号化する自己同期型ストリーム暗号化装置101（送信側）及び暗号化されたストリーム（暗号文）を復号する自己同期型ストリーム復号化装置110（受信側）を備える。これら暗号化装置101及び復号化装置110は、暗号通信を行う当事者が使用する端末に備えることができ、一方の当事者の端末に備えられた暗号化装置101によって暗号化された平文が、他方の当事者の端末に送信され、その復号化装置110によって復号化される。これらの装置は、専用のハードウェアによっても、また汎用のハードウェア及びその上で稼働されるプログラムによっても実現できることは、当業者であれば明らかであろう。

40

【0018】更に本発明は、前記自己同期型ストリーム暗号の暗号化装置と前記自己同期型ストリーム暗号の復号化装置を備えて構成される自己同期型ストリーム暗号システムである。

【0019】また、本発明は、前記自己同期型ストリーム暗号の暗号化装置を用いて N ビットの平文から S ビットのメッセージ認証子を生成するMAC生成方法であって、前記シフトレジスタに所定の初期値を設定する手順と、前記暗号化装置に N ビットの平文を入力する手順と、前記暗号化装置から出力された N ビットの暗号文の末尾から連続する S ビットをメッセージ認証子として出力する手順とを備えて構成される。

【0020】本発明は、また、同期信号に同期して動作する複数段のシフトレジスタと、多ビット入力1ビット出力の非線形変換計算部と、 n ビットの暗号化鍵を格納する暗号化鍵設定部とを有し、前記同期信号に同期して、平文を1ビットずつ入力し、暗号文を1ビットずつ

50

【0023】前記暗号化装置101及び復号化装置110は、それぞれ同じ構造のシフトレジスタ102、111、及び非線形変換計算部104、113を備える。こ

(5)

特開2001-16197

7

8

れらは、端末内のハードウェア構成として共用することができる。

【0024】暗号化装置101は、シフトレジスタ102、暗号化鍵設定部103、非線形変換計算部104及び排他的論理和演算部105～106を備える。暗号化装置101では、平文 P_i がビット毎に入力されると、同期信号に同期して暗号文 C_i がビット毎に出力される。すなわち、平文 P_i と非線形変換計算部104の出力は、排他的論理和演算部107でビット毎に排他的論理和演算され、その結果は暗号文 C_i として出力されると共に、シフトレジスタ102の最右段に入力される。シフトレジスタ102は、同期信号に同期してその記憶している内容を1ビット左シフトする。排他的論理和演算部105～106は、シフトレジスタ102の各段におけるレジスタ値に対して、暗号化鍵設定部103に設定された値を、ビット毎に排他的論理和するものである。非線形変換計算部104は、前記排他的論理和演算部105～106の各結果を入力し、それらを非線形変換し、結果として1ビットを出力する。

【0025】一方、復号化装置110は、シフトレジスタ111、復号化鍵設定部112、非線形変換計算部113及び排他的論理和演算部114～115を備える。復号化装置110では、受信した暗号文 C_i がビット毎に入力されると、同期信号に同期して平文 P_i がビット毎に出力される。すなわち、暗号文 C_i と非線形変換計算部113の出力は、排他的論理和演算部116でビット毎に排他的論理和演算され、その結果は平文 P_i として出力される。また、復号化装置110では、受信した暗号文 C_i は、シフトレジスタ111の最右段に入力される。シフトレジスタ111は、同期信号に同期してその記憶している内容を1ビット左シフトする。排他的論理和演算部114～115は、シフトレジスタ111の各段におけるレジスタ値に対して、復号化鍵設定部112に設定された値を、ビット毎に排他的論理和するものである。非線形変換計算部113は、前記排他的論理和演算部114～115の各結果を入力し、それらを非線形変換し、結果として1ビットを出力する。

$$k = (k_1, \dots, k_n), k_j \in \{0,1\}, (1 \leq j \leq n)$$

とすれば、

【0033】

【式5】

$$x_i = s_i \oplus k$$

である。ただし、

【0034】

【式6】

$$s_i \oplus k = (s_{i,1} \oplus k_1, \dots, s_{i,n} \oplus k_n)$$

であり、

【外1】

*【0026】ここに、非線形変換計算部104、113は、ベント(Bent)関数と呼ばれる多ビット(偶数ビット)入力1ビット出力のブール関数で構成される。ベント関数の一例を符号200として図2に示す。図において、204～207を通じて入力されたビット値は、論理積演算部201、202で演算された後に、排他的論理和演算部203に入力され、その結果は208に出力される。

【0027】このように構成された自己同期型ストリーム暗号方式が、ある鍵によって生成された暗号文の系列を異なる鍵で復号した場合の系列が、平文の系列と比較した場合、その相互相関が極めて小さくなる。この理由を以下に示す。

【0028】いま、図1の自己同期型ストリーム暗号システムにおける暗号化装置101において、時刻*i*において入力される平文を P_i 、出力される暗号文を C_i 、シフトレジスタ102の出力を、

【0029】

【式1】

$$s_i = (s_{i,1}, \dots, s_{i,n}), s_{i,j} \in \{0,1\}, (1 \leq j \leq n)$$

で表し、ベント関数である非線形変換計算部104の入力を、

【0030】

【式2】

$$x_i = (x_{i,1}, \dots, x_{i,n}), x_{i,j} \in \{0,1\}, (1 \leq j \leq n)$$

出力を、

【0031】

【式3】

$$z_i = f(x_i) \in \{0,1\}$$

で表したとする。但し、 n は偶数である。このとき、暗号化鍵設定部103に設定される暗号化鍵を、

【0032】

【式4】

40

⑧

は排他的論理和演算を示す。また、暗号文 C_i は、

【0035】

【式7】

$$c_i = p_i \oplus f(x_i) = p_i \oplus z_i$$

によって計算される。これら暗号文がシフトレジスタ102に入力されるため、シフトレジスタ102においては、その内部状態は、

【0036】

【式8】

50

$$s_i = (c_{i-1}, \dots, c_{i-n})$$

(6)

特開2001-16197

9

10

と表すことができる。いま、平文 P_i 同士が統計的にランダムであり、時間的にも相関が全くないと仮定すると、式7より、暗号文 C_i 同士も統計的にランダムとなり、また、時間的にも相関がないことになる。これは、いかなる情報源からの系列であってもランダムな情報源からの系列と排他的論理和演算を施せばランダムな系列となるという事実に容易に理解できる。

【0037】復号化装置110において、時刻*i*におけるシフトレジスタ111の出力を、暗号化装置101と同様に、式1. ベント関数である非線形変換計算部113の入力を式2. 出力を式3で表したとする。また、復号化鍵設定部112に設定される復号化鍵は、暗号化鍵と同じ値、すなわち式4とする。このとき、平文 P_i は次のように復号化される。

【0038】

【式9】

$$P_i = C_i \oplus Z_i = C_i \oplus f(X_i)$$

における1、0の出現頻度によって観測することができる。特に、1、0の出現頻度が等しければ相互相関はないことになる。式13は、

【0043】

【式14】

$$(C_{i-1} \oplus K_1, \dots, C_{i-2} \oplus K_n) = (u_{i-1}, \dots, u_{i-2}) = u_i$$

※

$$b = (b_1, \dots, b_n) = (K_1 \oplus K'_1, \dots, K_n \oplus K'_n)$$

である。ここに、 f はベント関数である。ベント関数においては、以下の性質が知られている。すなわち、ベント関数*f*においては、

【0046】

【式17】

$$\sum_{x \in \{0,1\}^n} f(x) \oplus f(x \oplus a) = 2^{n-1}$$

なる性質がある。但し、 $a \in \{0, 1\}^n$ 、 $a \neq \{0, 0, \dots, 0\}$ である。この事実は、Seongrack Chee, Sangjin Lee, Kwangjo Kim著の論文、"Semi-bent functions, Advances in Cryptology ASIACRYPT'94, LNCS 914, Springer-Verlag, pp.107-118, 1995"等に記されている。

【0047】前記の事実に踏まえた上で、前に述べたように、平文 P_i 同士が統計的にランダムであり、時間的にも相関が全くないと仮定すると、 C_1, \dots, C_n は統計的にランダムであり、時間的にも相関が全くないことになるから、式15における u_i もランダムとみなせることになる。したがって、式15に式17の結果を適用することにより、

【0048】

【式18】

* 式9に、式5、式6及び式8を適用すれば、次式を得る。

【0039】

【式10】

$$P_i = C_i \oplus f(C_{i-1} \oplus K_1, \dots, C_{i-2} \oplus K_n)$$

いま、復号化鍵設定部112に、暗号化に用いた鍵と異なる鍵、

【0040】

【式11】

$$K' = (K'_1, \dots, K'_n), K'_j \in \{0, 1\}, (1 \leq j \leq n)$$

を設定したとする。このとき、復号化装置110の出力 P'_i は次式のように表される。

【0041】

【式12】

$$P'_i = C_i \oplus f(C_{i-1} \oplus K'_1, \dots, C_{i-2} \oplus K'_n)$$

ここに P_i と P'_i の相互相関は、

【0042】

【式13】

* とおくことにより、次式となる。

【0044】

【式15】

$$P_i \oplus P'_i = f(u_i) \oplus f(u_i \oplus b)$$

ただし、

【0045】

※

【式16】

30

$$\sum_{i=1}^n P_i \oplus P'_i = \sum_{i=1}^n f(u_i) \oplus f(u_i \oplus b) = 2^{n-1}$$

が得られる。これは、ある鍵によって生成された暗号文の系列を異なる鍵で復号した場合の系列が、前記暗号文の生成に用いた平文の系列と比較した場合、その相互相関が極めて小さくなることを示す。

【0049】次に、図3は、前記自己同期型ストリーム暗号システムにより生成されるMACを示したものである。図において符号300は、前記自己同期型ストリーム暗号システム100によって、平文*N*ビットから生成された*N*ビットの暗号文である。該暗号文300において、その末尾から連続する*S*ビット部分301をMACとして用いることができる。

【0050】以上、本発明の一実施形態を図面に沿って説明した。しかしながら本発明は前記実施形態に示した事項に限定されず、特許請求の範囲の記載に基いてその変更、改良等が可能であることは明らかである。例えば、前記非線形変換計算部は、鍵設定部の値がそのベント関数へ入力される限り、以下のように構成しても良

50 い。

(7)

特開2001-16197

11

12

(1) 非線形変換計算部のベント関数には、シフトレジスタと排他的論理和の結果以外への入力。例えば、シフトレジスタの他のビット値を入力しても良い。
 (2) 非線形変換計算部の出力は、ベント関数による演算結果と他の演算結果を排他的論理和したものとしても良い。

【0051】

【発明の効果】以上の如く本発明によれば、ある鍵によって生成された暗号文の系列を異なる鍵で復号した場合の系列が、平文の系列と比較した場合、その相互相関が極めて小さくなり、かつ、鍵の設定が容易であるような自己同期型ストリーム暗号システムを提供することが可能になる。

【図面の簡単な説明】

【図1】本発明に係る自己同期型ストリーム暗号システムの一実施形態を示すブロック図である。

【図2】ベント関数の一例を示すブロック図である。

【図3】本発明に係る自己同期型ストリーム暗号システムにより生成されるMACを示した図である。

【図4】従来の自己同期型ストリーム暗号システムのブ*20

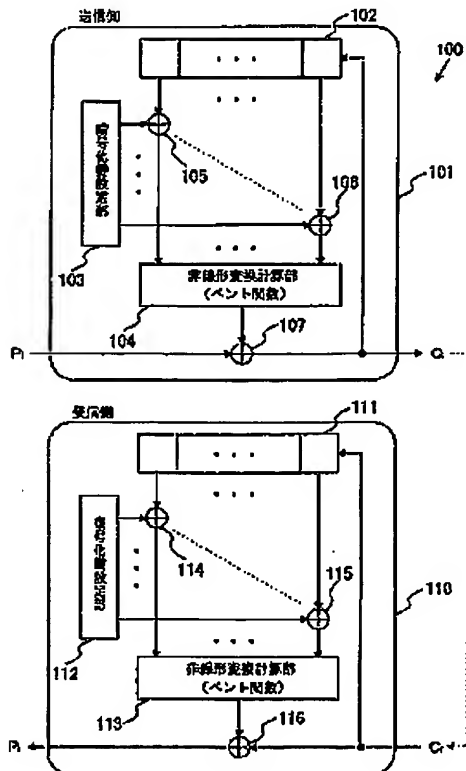
* ロック図である。

【図5】ブロック暗号方式におけるCBCモードを示す図である。

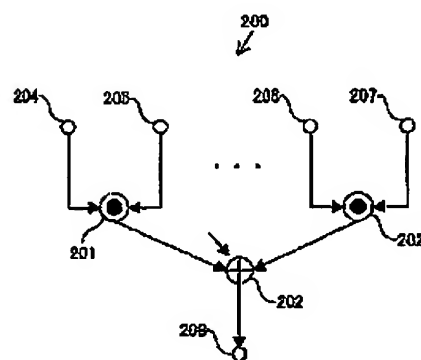
【符号の説明】

100 自己同期型ストリーム暗号システム
 101 自己同期型ストリーム暗号化装置
 102 シフトレジスタ
 103 暗号化鍵設定部
 104 非線形変換計算部
 105～106 排他的論理和演算部
 107 排他的論理和演算部
 110 自己同期型ストリーム復号化装置
 111 シフトレジスタ
 112 復号化鍵設定部
 113 非線形変換計算部
 114～115 排他的論理和演算部
 116 排他的論理和演算部
 201、202 論理積演算部
 203 排他的論理和演算部

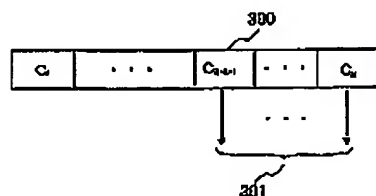
【図1】



【図2】



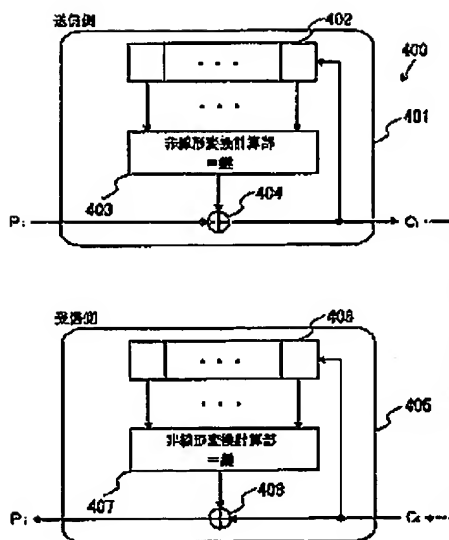
【図3】



(8)

特開2001-16197

【図4】



【図5】

